this growing international concern was exemplified by the nomination of the Roman Catholic Bishop of East Timor, 47-year-old Carlos Ximenes Belo, for the Nobel Peace Prize. The Associated Press and other news organizations listed Bishop Belo as a finalist in the days before the peace prize winner was announced in mid-October.

As one of those who nominated Bishop Belo for the Nobel Peace Prize, I firmly believe that the Congress and the Clinton administration and other governments and parliaments and world leaders should support Bishop Belo in his continuing efforts to ward off violence and find a just, peaceful solution to the East Timor tragedy under U.N. auspices.

It is crucial that Bishop Belo receive the maximum possible international support for his heroic efforts. In the year to come, I will work with my colleagues to help ensure that he gets it.

COMPUTER PRIVACY

HON. BOB GOODLATTE

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, December 6, 1995

Mr. GOODLATTE. Mr. Speaker, I rise today to bring to the attention of all Members of Congress, action being taken by the administration which threatens the personal privacy of everyone using a computer. Let me explain.

Even before Julius Caesar began dispatching runners with coded messages, governments and private citizens have searched for ways to protect vital personal and business secrets. As communications have become more sophisticated, so too have the methods used to secure private and confidential communications. Information sent by computer today is often protected by ''encryption'' technology. The technology applies a mathematical equation which scrambles data so it can only be read by the person holding the ''key'' which unscrambles the information. For years, the Government has argued that it should hold a ''key'' to everyone's computer—you may recall the ''clipper chip'' debate during the last Congress.

Despite the wholehearted rejection of the clipper chip, the Government is back at it. Yesterday, the National Institute of Standards and Technology [NIST] held a hearing on an administration proposal called the ''64-bit software key escrow encryption export criteria.'' Beyond this technical jargon, this appears to be a very dangerous proposal; some are referring to it as the ''son of clipper.'' The new proposal is opposed by a wide range of interests, including the high-technology industry, free speech advocates, and free-market groups.

The Ad Hoc Taxpayer Coalition for Computer Privacy, which includes Americans for Tax Reform, and Citizens for a Sound Economy, says this proposal is anticonsumer, antimarketplace, anti-American business, and antiprogress. A group of three dozen high-tech business interests have informed the administration that they will attempt to craft their own policy because the administration's just misses the boat. Mr. Speaker, I ask unanimous consent to insert letters from these two groups in the CONGRESSIONAL RECORD as well as letters from the Business Software Alliance, the Information Technology Association of America, and the Information Technology Industry Council.

Mr. Speaker, it appears that the administration is trying to set a national policy on computers without a true public hearing. Such serious issues should not be resolved behind closed doors or at obscure hearings. Congress is being called upon to become involved in the debate over a national encryption policy. I think we should take a close look at this and I urge my colleagues to consider this seriously.

THE AD HOC TAXPAYER COALITION
FOR COMPUTER PRIVACY,
November 8, 1995.

Hon. NEWT GINGRICH,
Speaker of the House of Representatives, The Capitol, Washington, DC.

DEAR MR. SPEAKER: We are writing to express serious concerns about the Administration's efforts to continue to restrict the ability of computer users at home and abroad to protect their personal and private information over electronic networks through the use of encryption technology. The Administration seems determined to ensure government surveillance of all electronic information and communications. It began with President Clinton's ''Clipper Chip,'' but has not stopped.

Consumers aren't happy with these proposals, and neither is the business community nor civil libertarians. In fact, it's hard to find anyone supportive outside the Administration except for the few that would benefit from the Administration's ''proposed relaxation'' of the nation's export policy.

The Administration refuses to let American computer hardware and software companies sell products with good encryption worldwide unless the U.S. Government is guaranteed access to a key that unlocks that information. The Administration is trying to leverage these companies' need to export—they derive more than half their earnings from sales abroad—and desire to develop a single product worldwide, to force them to include a feature in products they sell in the U.S. and abroad that will allow government access. Administration officials also have said that if American companies do not ''voluntarily'' include such a feature, then they will seek legislation making such a feature mandatory.

The Administration's approach is the wrong policy for today's marketplace.

It's anti-consumer. Computer users will not entrust their sensitive information to computer networks unless its security and privacy are assured. Without good privacy protection, there simply will not be a Global Information Infrastructure—and America won't be in the lead.

It's anti-marketplace. There is no consumer demand for encryption products that give the government easy access. The Administration has come forward with a typical big-government approach—a government designed solution for a government problem. This completely overlooks the realities of a free-market.

It is anti-American business. The Administration's current policies are seriously harming the continued competitiveness of one of our fastest growing and most successful industries—the computer hardware and software industry. Computer users are demanding good encryption but American companies are not allowed to supply it. Yet there are hundreds of foreign encryption products manufactured and encryption programs are widely available on the Internet.

Finally, it is anti-progress. Wishing that there was no encryption available will not make it so. The technology is widely understood and available—you can't put this genie back in the bottle. Government policies should not encumber the American computing industry as it leads the world technology revolution.

We strongly urge you to oppose attempts to limit the ability of Americans to use whatever encryption they wish and to support the immediate relaxation of harmful export controls on American products and programs with encryption features.

Americans for Tax Reform; Association of Concerned Taxpayers; Competitive Enterprise Institute; Citizens for a Sound Economy; The Business Leadership Council; The Small Business Survival Committee; Citizens Against a National Sales Tax/VAT.

Virginia Postrel, Editor, Reason magazine; Sheldon Richman, Senior Editor, The Cato Institute; Tanya Metaksa, Executive Director, Institute for Legislative Action, National Rifle Association; Kellyanne Fitzpatrick, The Polling Company; and Donna Matias, Institute for Justice.

NOVEMBER 8, 1995.

Hon. ALBERT GORE, Jr.,
Office of the Vice President, Old Executive Office Building, Washington, DC.

DEAR MR. VICE PRESIDENT: A secure, private, and trusted Global Information Infrastructure (GII) is essential to promote economic growth and meet the needs of the Information Age society. Competitive businesses need cryptography to protect proprietary information as it flows across increasingly vulnerable global networks. Individuals require privacy protection in order to build the confidence necessary to use the GII for personal and financial transactions. Promoting the development of the GII and meeting the needs of the Information Age will require strong, flexible, widely-available cryptography. The undersigned groups recognize that the Administration's recently articulated cryptography initiative was a serious attempt to meet some of these challenges, but the proposed initiative is no substitute for a comprehensive national cryptography policy. To the extent that the current policy becomes a substitute for a more comprehensive policy, the initiative actually risks hindering the development of a secure and trusted GII.

A number of the undersigned organizations have already written to express concern about the latest Administration cryptography initiative. As some of us have noted, the Administration's proposed export criteria will not allow users to choose the encryption systems that best suit their security requirements. Government ceilings on key lengths will not provide an adequate level of security for many applications, particularly as advances in computing render current cryptography systems less secure. Competitive international users are steadily adopting stronger foreign encryption in their products and will be unlikely to embrace U.S. restrictions. As they stand, current export restrictions place U.S. hardware manufacturers, software developers, and computer users at a competitive disadvantage, seriously hinder international interoperability, and threaten the strategically important U.S. communications and computer hardware and software industries. Moreover, the Administration policy does not spell out any of the privacy safeguards essential to protect individual liberties and to build the necessary public trust in the GII.

The current policy directive also does not address the need for immediate liberalization of current export restrictions. Such liberalization is vital to enable U.S. companies to export state-of-the-art software products

during the potentially lengthy process of developing and adopting a comprehensive national cryptography policy. Without relief, industry and individuals alike are faced with an unworkable limit on the level of security available and remain hamstrung by restrictions that will not be viable in the domestic and international marketplace.

Many members of the undersigned groups have been working actively with the Administration on a variety of particular applications, products, and programs promoting information security. All of us are united, however, by the concern that the current network and information services environment is not as secure as it should be, and that the current policy direction will delay the secure, private, and trusted environment that is sought.

Despite the difficulties of balancing the competing interests involved, the undersigned companies, trade associations, and privacy organizations are commencing a process of collective fact-finding and policy deliberation, aimed at building consensus around a more comprehensive cryptography policy framework that meets the following criteria:

Robust security: access to levels of encryption sufficient to address domestic and international security threats, especially as advances in computing power make currently deployed cryptography systems less secure.

International interoperability: the ability to securely interact worldwide.

Voluntary use: freedom for users to choose encryption solutions, developed in the marketplace, that meets their particular needs.

Acceptance by the marketplace: commercial viability and ability to meet the expressed needs of cryptography users.

Constitutional privacy protections: safeguards to ensure basic Fourth amendment privacy protection and regulation of searches, seizures, and interceptions.

Respect for the legitimate needs of law enforcement and national security while recognizing the reality that determined criminal will have access to virtually unbreakable encryption.

In six months, we plan to present our initial report to the Administration, the Congress, and the public in the hopes that it will form the basis for a more comprehensive, long-term approach to cryptography on the GII. We look forward to working with the Administration on this matter.

Sincerely,

American Electronics Association; America Online, Inc.; Apple Computer, Inc.; AT&T; Business Software Alliance; Center for Democracy & Technology; Center for National Security Studies; Commercial Internet Exchange Association; CompuServe, Inc.; Computer & Communications Industry Association; Computing Technology Industry Association; Crest Industries, Inc.; Dun & Bradstreet; Eastman Kodak Company; Electronic Frontier Foundation; Electronic Massaging Association; ElijaShim Microcomputers, Inc.; Formation, Inc.

Institute for Electrical and Electronic Engineers—United States Activities; Information Industry Association; Information Technology Industry Council; Information Technology Association of America; Lotus Development Corporation; MCI; Microsoft Corporation; Novell, Inc.; OKIDATA Corporation; Oracle Corporation; Securities Industry Association; Software Industry Council; Software Publishers Association; Software Security, Inc.; Summa Four, Inc.; Sybase, Inc.; Tandem Computers, Inc.; Telecommunications Industry Association; and ViON Corporation.

BUSINESS SOFTWARE ALLIANCE,
Washington, DC, November 9, 1995.

Hon. ALBERT GORE,
Vice President of the United States, The White House, Washington, DC.

DEAR MR. VICE PRESIDENT: Last summer our member companies Chief Executive Officers and I wrote you expressing the American software industry's most serious concern about the continuing inability to export generally available software programs with the encryption capabilities customers worldwide demand. We also conveyed BSA's extreme disappointment about the lack of consultation with industry regarding the development of so-called key escrow encryption approaches.

On August 17th, the Administration announced its most recent decisions on encryption policy. We learned more about the Administration's approach in discussions with members of the Interagency Working Group on Encryption and at three days of presentations and discussions at NIST. This Monday, November 6th, NIST published further defined, yet essentially unchanged criteria for the export of software-based key escrow encryption.

After careful and serious deliberation by our members, we have concluded that the Administration's approach is fatally flawed and cannot be the basis for progress in this area. Instead, we strongly urge the Administration to:

1. Separate export control issues from national encryption policy.

American software companies seek to develop, market and sell a single version of their program worldwide. The Administration appears to be trying to leverage our companies' desire to export their programs in order to force those companies to include features in the programs they sell abroad and in the U.S. that will permit government access to encrypted information, even though such features are commercially undesirable and there is no current requirement that they be employed by domestic users. Thus, in the name of ''national security,'' it appears that the Administration really is attempting to satisfy domestic law enforcement concerns—without industry input, public debate or congressional involvement. We urge you not to let export control policy dictate national encryption policy.

2. Immediately permit the export of generally available software programs employing the Data Encryption Standard (DES) algorithm or other algorithms at comparable strengths, provided information about the program is submitted to NSA under a strict non-disclosure arrangement. Also, thereafter increase automatically the permissible key length two bits every three years given that the computing power for the same cost doubles every 18 months (i.e. institute a ''COCA'' or ''Cost Of Cracking Adjustment'').

American software companies have been forced to continue limiting the strength of their encryption to the 40-bit key length level. But this outdated level ignores the fact that the DES algorithm with 56-bit key lengths is the current worldwide standard. It ignores the serious vulnerability of 40-bit encryption to successful commercial attack by those employing commercially available resources (e.g. the successful hacking of Netscape). It ignores the availability of hundreds of alternatives from scores of foreign manufacturers.

Additionally, it ignores the fact that all proposed Internet Protocols addressing security call for an encryption standard at least at the DES level. The backbone of the Global Information Infrastructure (GII) is the Internet. In the last few years, American companies have adapted their business plans to work with the realities of the Internet. Companies wishing to provide software for, or do business on, the Internet must acknowledge such standards if they are to have any chance of gaining widespread acceptance. Finally, the 40-bit key length ignores the ability of NSA to decode encryption with longer keys (through brute force attacks and other approaches because of their intimate knowledge of the programs) and thereby to protect national security.

3. Work with industry, privacy groups and Congress on a comprehensive national encryption policy.

The digital information age and GII present opportunities and challenges to computer users concerned about privacy at home and in their businesses, as well as law enforcement agencies. We appreciate and respect law enforcement needs—but, in turn, the FBI and other agencies should understand the nature and evolution of computer networks and the needs and desires of computer users for reliable, flexible and trustworthy information security features. There must be an open public debate. Congress should be involved. Information security policies for the electronic world are fundamental to the success of the GII and are too important to be addressed behind closed doors at secret agencies.

Sincerely,

ROBERT W. HOLLEYMAN II,
President.

INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA,
Arlington, VA, September 27, 1995.

Hon. AL GORE,
Vice President of the United States, Washington, DC.

DEAR MR. VICE PRESIDENT: The ability of companies and individuals to ensure that the information they send over communications networks is secure is a prerequisite to exploiting the potential of the Global Information Infrastructure. It will have a large impact on the ability of U.S. firms to compete in the global marketplace and create jobs here.

While the Administration has been a forceful and effective advocate of the Global Information Infrastructure, its restrictive policies on the export of encryption technology has created a major barrier to realizing the Administration's vision.

The Information Technology Association of America (ITAA) believes that the Administration's key escrow encryption proposal announced on August 17, 1995 has some fundamental flaws.

Most significantly, the Administration's proposal misses the reality that a de facto global standard exists today, and that standard is DES: a 56 bit, encryption method that is used without any key escrow requirements. Increases in computational power are causing consumers to look for strong encryption and 40-bit key lengths have been broken recently. DES is widely available throughout the world, and many end-users are demanding security for their communications beyond this 56 bit standard. That is, end-users' confidence in 56 bit encryption is weakening and even DES may soon be obsolete. These realities are market-driven and will not change as a result of U.S. government intervention.

Given these market realities, the Administration should decontrol immediately the export of 64 bit key length encryption software with no strings attached. Even this level of decontrol will have to be addressed again in the not too distant future given the march of technology and rapid increases in computing power.

In addition, if industry were to agree to the government's requirement to invest in and build a potentially expensive and technically complicated escrow scheme in exchange for the right to export, non-escrow technology could be placed at a disadvantage in the domestic marketplace. Such a development could suppress technological innovation and slow development of more powerful levels of information security.

Finally, we do not think it is necessary to mandate that a number of commercial companies will gain the right to qualify as escrow key agents. We see no reason why organizations could not hold their own keys.

Just as the Cold War dictated that the nation engage in a costly defense against a real threat, so must U.S. industry be allowed to arm itself with encryption protection strong enough to meet the known threat to our industrial and economic security. We look forward to working with the Administration to ensure that the U.S. policy on encryption balances both economic and national security interests.

ITAA represents more than 6,500 members and affiliates throughout the United States. High technology industry segments represented in our membership include software, telecommunications, services, systems integrators and computers. Many of these companies are international and view their markets as global.

Thank you for considering our comments. If you have any questions, please contact me at 703–284–5301 (telephone) or hmiller@itaa.org (e-mail).

Sincerely,

HARRIS N. MILLER,
President.

INFORMATION TECHNOLOGY
INDUSTRY COUNCIL,
Washington, DC, October 10, 1995.

Hon. ALBERT GORE, Jr.,
Office of the Vice President, Old Executive Office Building, Washington, DC.

DEAR MR. VICE PRESIDENT: I am writing on behalf of the Information Technology Industry Council to let you know our views on the Administration's recent encryption proposal. ITI represents the leading U.S. providers of information technology products and services. Our members had worldwide revenue of $323 billion in 1994 and employ more than one million people in the United States. It is our member companies that are providing much of the hardware, software, and services that are making the ''information superhighway'' a reality.

ITI applauds your efforts to further develop U.S. policy on export of encryption technologies and your willingness to hear from the private sector on your recent proposal. However, ITI believes the proposal does not adequately meet the needs of industry or users, nor does it sufficiently recognize the importance of information security to economic growth and industrial society in the information age. Specifically, the proposed criteria will restrict users' freedom to choose the encryption that best meets their security needs and the key management system appropriate to those needs, will not allow users to maintain and manage their own keys, ignores the steady improvements in the ability of competitive foreign firms to incorporate strong security features in their products and services, and will be difficult to implement internationally. The proposed interoperability criteria will make it more difficult for domestic users to use non-key escrow encryption in the United States. Systems that do not interoperate are not attractive to domestic and international customers with significant installed bases and are contrary to your own definition of the information superhighway as a ''seamless web of communications networks, computers, databases, and consumer electronics . . .''.

It appears that the proposed export criteria are driven solely by the views of law enforcement and national security agencies, without taking into account the needs of commercial users. While law enforcement and national security goals are important, export restrictions that do not reflect marketplace realities may drive U.S. companies to move their encryption work off shore, resulting in the loss of an important domestic technology base, as well as defeating the very purpose of the restrictions.

As you work to finalize the export criteria, we urge you to also immediately decontrol the export of commercial software, at least to allow the export of products including the Data Encryption Standard (DES), which has become the global standard for business and personal use.

We are further concerned about the accelerated effort to develop Federal key escrow standards. The Federal Information Processing Standards appear designed to establish de facto private sector computer security standards. FIPS, which are designed to meet specific government needs, should not drive national policy on information infrastructure, law enforcement, security, and export control. With so many fast-breaking commercial developments in this area, it is far from clear what technologies will emerge from the marketplace. If the FIPS process proceeds too quickly, the government may end up adopting standards that are incompatible with those used in international commercial markets.

ITI looks forward to working with the Administration to develop a national cryptography policy that provides law enforcement and national security agencies with due process access, but which also meets the interoperable security needs of the GII. ITI is continuing to develop specific comments on the proposed export criteria, which we will detail in a follow-up letter to your staff. In the meantime, we hope you will consider these comments as you continue to refine your encryption proposals.

Sincerely,

RHETT DAWSON,
President.

AN INDEPENDENT KHALISTAN

HON. PHILIP M. CRANE

OF ILLINOIS

IN THE HOUSE OF REPRESENTATIVES

Wednesday, December 6, 1995

Mr. CRANE. Mr. Speaker, I rise today to inform my colleagues, the American people, and the international community about the recent surge of activity that has occurred in this town regarding the Sikh struggle for an independent Khalistan.

On October 19, 1995, 65 Members of Congress signed a letter to Indian Prime Minister P.V. Narasimha Rao demanding the release of Sikh human rights activist Jaswant Singh Khalra. Mr. Khalra was abducted by Indian police in front of his home on September 6. It appears that Mr. Khalra represents a threat to the Indian Government because he had recently published a report in which he estimated that Indian police in Punjab, working under the direction of the Indian Government, had abducted murdered, and cremated over 25,000 Sikhs. Sikhs have long accused the Indian police in Punjab of conducting their terror campaign against the Sikhs according to this modus operandi. Mr. Khlara confirmed these accusations by tallying up the so-called unidentified bodies registered in municipal cremation grounds throughout Punjab. It should be known that in Punjab, family networks are extremely tight which would leave rare occasion for someone to die and not have the body identified by the next of kin. In the Amritsar District alone, Mr. Khalra found 6,017 unidentified bodies registered in the municipal crematorium. These findings seem to support Mr. Khalra's claim that the Punjab police have been killing Sikh and cremating their remains as unidentified bodies in order to erase any evidence of police wrongdoing. Under these circumstances we can understand why Amnesty International states in its latest report, ''Determining the Fate of the 'Disappeared in Punjab,'' that ''the Punjab Police have been allowed to commit human rights violations with impunity.''

As a result of the letter of the 65 Members of Congress, President Clinton wrote a letter to Congressman GARY CONDIT, the initiator of the letter to express that he, too, is ''concerned by reports regarding Jaswant Singh Khalra.'' The President stated that the ''U.S. Embassy in New Delhi has already made inquiries into these allegations with various Indian Government agencies, and Ambassador Wisner has raiser the issue with high-ranking officials.''

Turning up the pressure on India even further, Congressman CONDIT is sending a letter to the Secretary General of the United Nations, Boutros-Boutros Ghali, in which he asks the United Nations to ''issue a strong statement condemning the murders of over 25,000 Sikhs'' and to ''demand the release of Mr. Khalra by India immediately.''

The media has been watching the congressional activity on behalf of the Sikhs closely. The November 28 issue of the Washington Times ran an article titled, ''Clinton checks India'', reporting on President Clinton's condemnation of India's abduction of Mr. Khalra. On November 3, the Washington Times also reported on an encounter between Dr. Gurmit Singh Aulakh, President of the Council of Khalistan and Indian Ambassador S.S. Ray which occurred in the halls of the Longworth House Office Building. Dr. Aulakh, the article reports, ''blames Mr. Ray for widespread human rights abuses when the ambassador was Governor of Punjab in the late 1980's. During that time thousands died in violence linked to Sikh demands for a separate homeland.'' When Dr. Aulakh encountered Mr. Ray in the Longworth building, he did not hestate to speak his mind. As the article quotes Dr. Aulakh: ''I walked up to him and told him, 'You are a murderer and should not be walking these halls.' ''

The efforts of Dr. Aulakh and the Council of Khalistan on behalf of the Sikh nation in its struggle for freedom from India have been highly successful. According to News India-Times, ''Sikh Nation activists led by Gurmit Singh Aulakh perhaps pose the biggest challenge and threat to India's lobbying efforts in the capital.'' Mr. Speaker, I would submit that the reason for the success of the Sikh nation in the U.S. Congress is due half in part by extremely hard work on the part of the Sikhs and half in part to the fact that evidence against India is so overwhelming. Though it claims to be a democracy, India is one of the most brutal regimes in the world regarding its dealings with minority nations and people under its rule.